Romain Jacquet **BTS SIO 1**

02/10/2025

Compte rendu TP 2 -B3-PIA

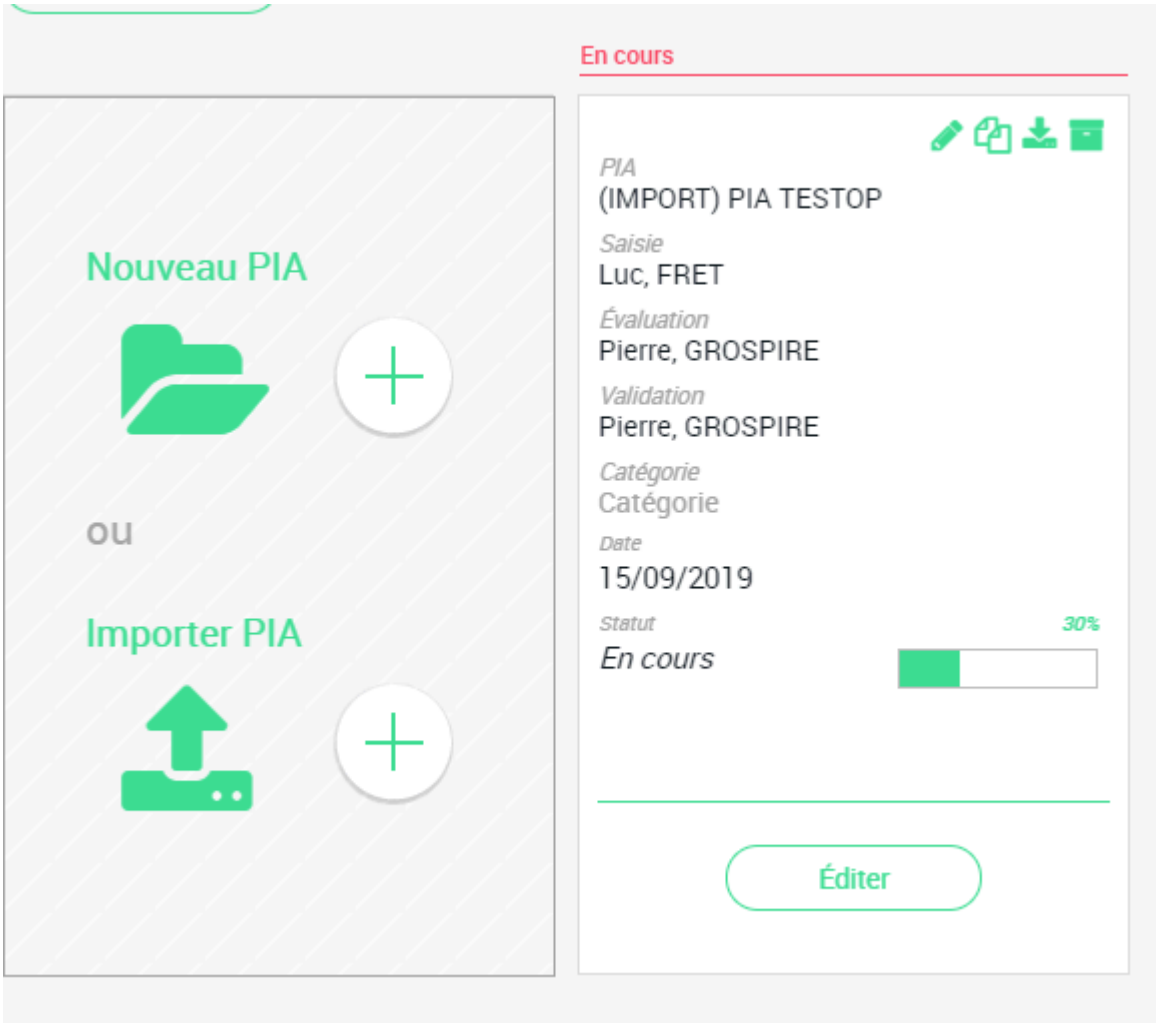
Sommaire

Introduction

Ce TP m'a permis de découvrir comment protéger les données personnelles et gérer les risques liés à leur traitement. À travers l'analyse d'un PIA, la cartographie des traitements et l'identification des données sensibles, j'ai pu comprendre concrètement les enjeux du RGPD et de la sécurité informatique.

Exercice 1.Analyser un PIA

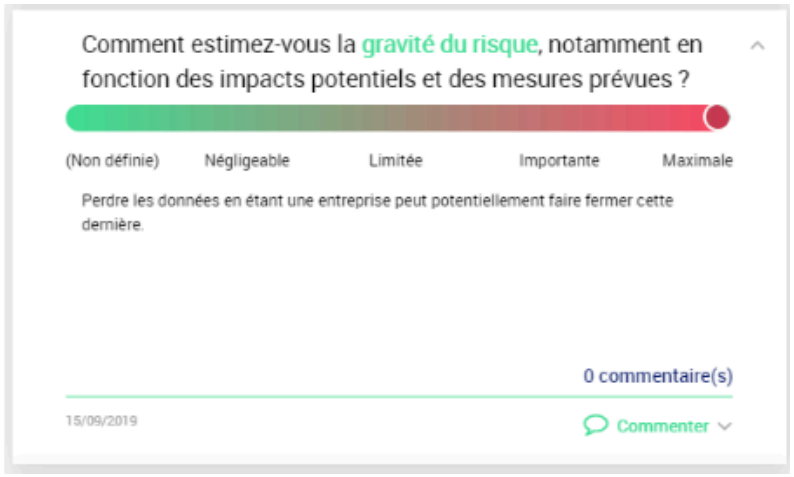
1)J'ai commencé par importer le travaille de M.Grospire sur l'application PIA

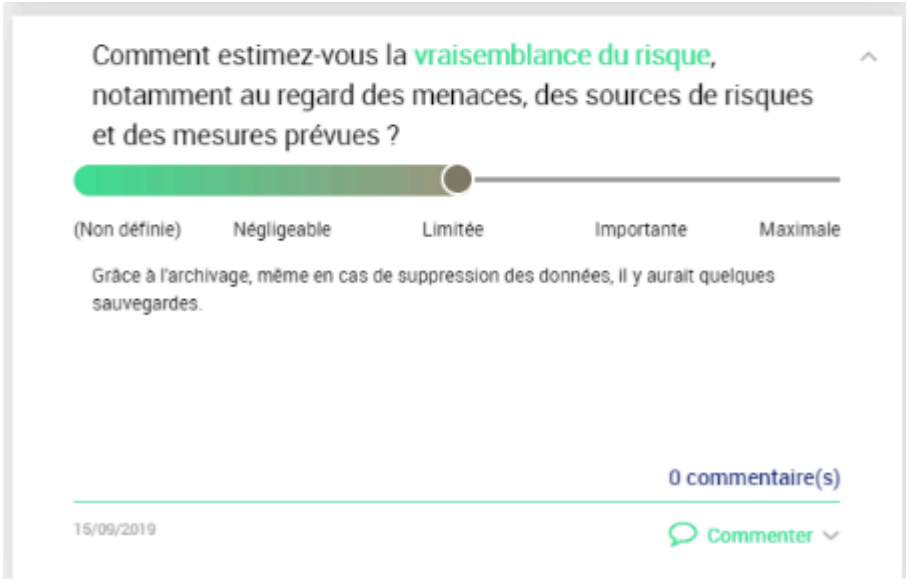


2)Pour l'accès illégitime à des données.

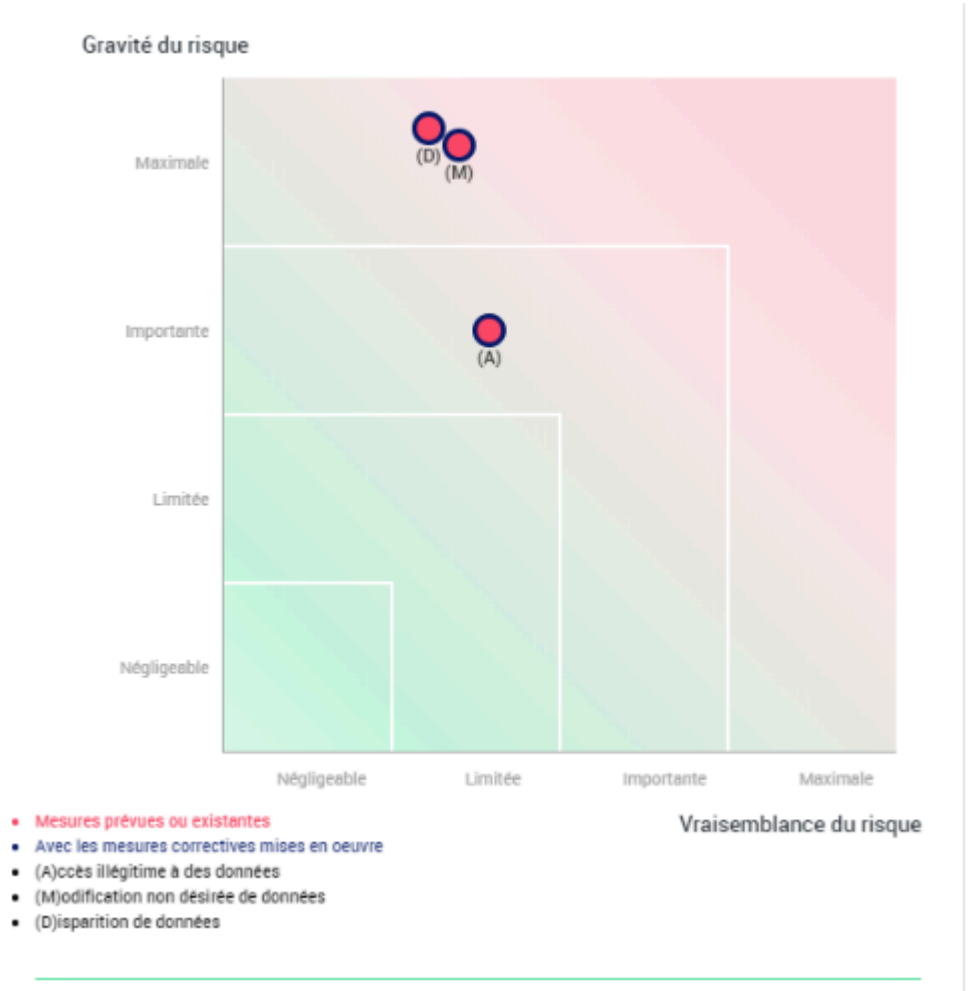
Pour le risque modification non désiré de donnée :

Pour le risque disparition de données

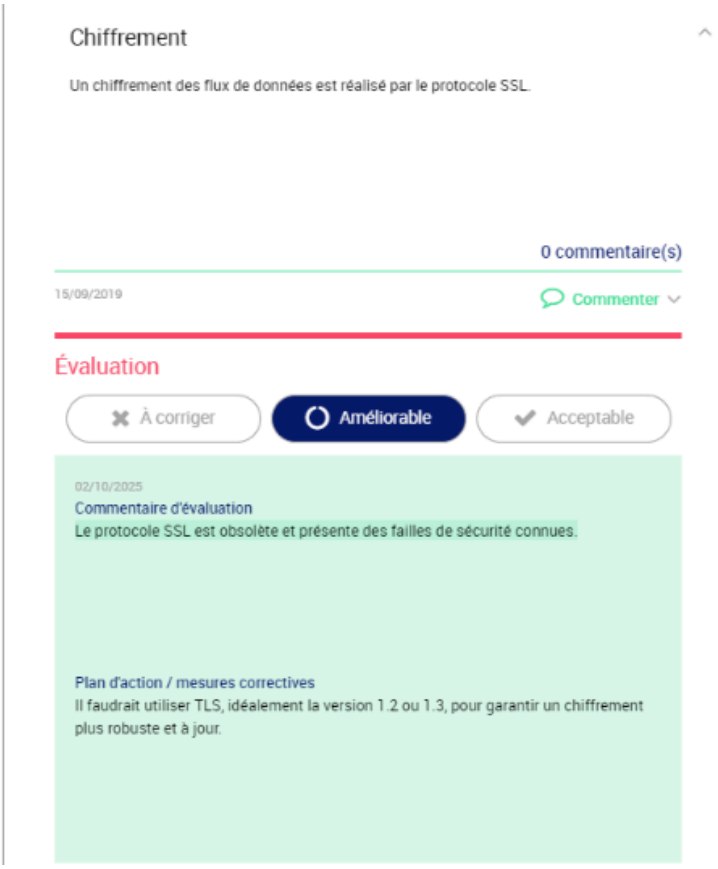




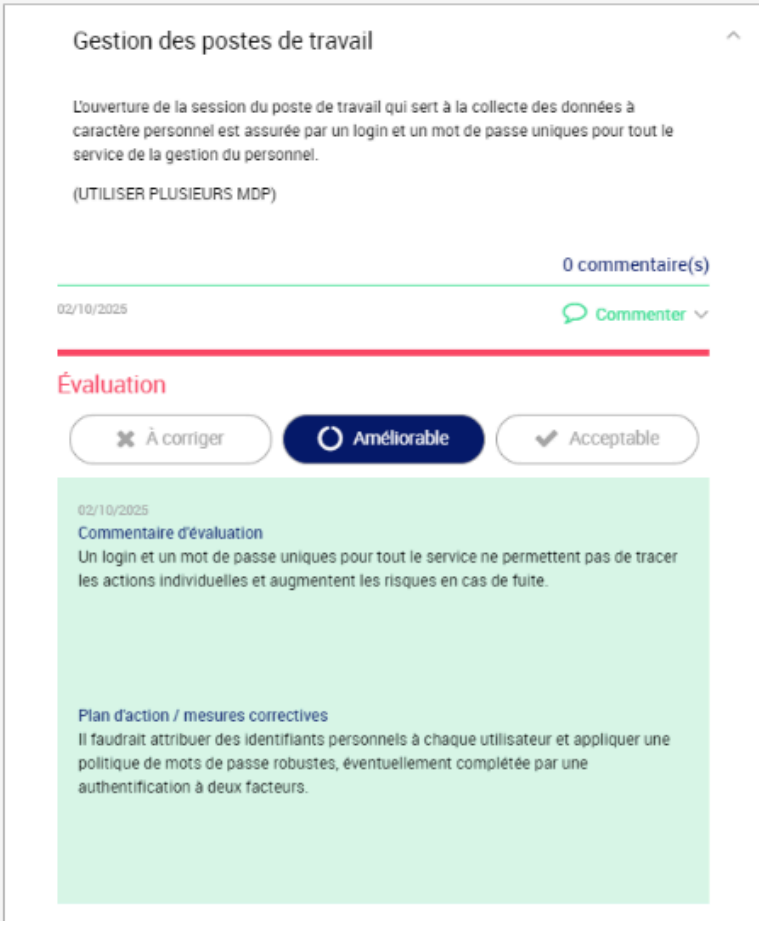
3) Pour le moment la cartographie des risques est la suivante :



4)LES MESURES EXISTANTES OU PRÉVUES :




Archivage
Les données sont sauvegardées sur un disque dur externe puis celui-ci est amené au service informatique pour le transfert dans une base de données de TESTOP et vers un serveur hébergé par la société OVH.
0 commentaire(s)
15/09/2019
Commenter
Évaluation
À corriger
Améliorable
Acceptable
02/10/2025
Commentaire d'évaluation
Le transfert manuel sur un disque dur externe présente des risques de perte ou de vol.
Plan d'action / mesures correctives
Il serait préférable d'utiliser un transfert sécurisé et automatisé (par exemple via SFTP ou un VPN) et de chiffrer les sauvegardes avant leur envoi vers le serveur hébergé par OVH.

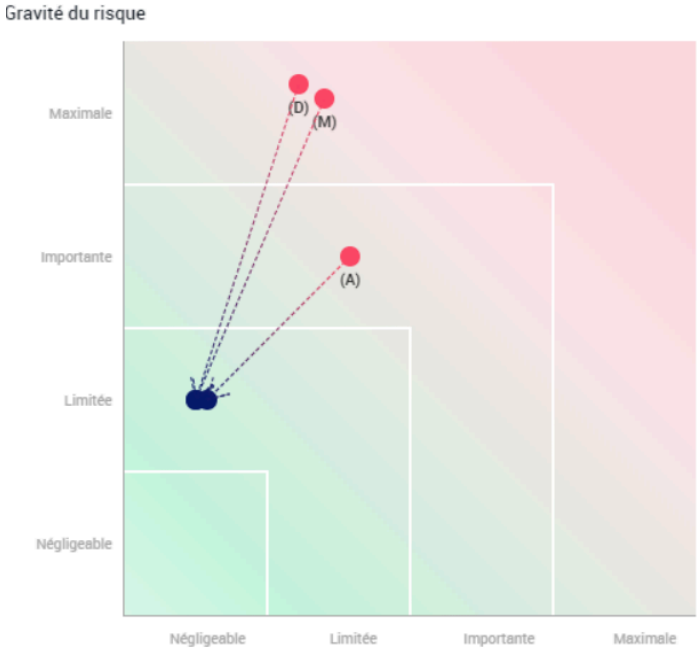

Gestion des postes de travail
L'ouverture de la session du poste de travail qui sert à la collecte des données à caractère personnel est assurée par un login et un mot de passe uniques pour tout le service de la gestion du personnel.
(UTILISER PLUSIEURS MDP)
0 commentaire(s)
02/10/2025
Commenter
Évaluation
À corriger
Améliorable
Acceptable
02/10/2025
Commentaire d'évaluation
Un login et un mot de passe uniques pour tout le service ne permettent pas de tracer les actions individuelles et augmentent les risques en cas de fuite.
Plan d'action / mesures correctives
Il faudrait attribuer des identifiants personnels à chaque utilisateur et appliquer une politique de mots de passe robustes, éventuellement complétée par une authentification à deux facteurs.

ACCÈS ILLÉGITIME À DES DONNÉES :

MODIFICATION NON DÉSIRÉES DE DONNÉES :

DISPARITION DE DONNEES :

5) Après avoir tout remplis, voici la cartographie des risques



Les risque sont toujours présent mais ils sont limité

Exercice 2 Cartographier le traitement des données à caractère personnel.

1) La cartographie des traitements de données personnelles est une étape clé pour toute organisation qui veut être en règle avec le RGPD. En gros, il s'agit de recenser, décrire et organiser tous les traitements de données personnelles effectués dans l'entreprise. Cela permet d'avoir une vue claire des données qui circulent, ce qui aide à mieux gérer les risques et à mettre en place des mesures de sécurité adaptées.

2) Avant tout, il est important de créer un registre des traitements de données personnelles. Cela permet de repérer les risques éventuels et de corriger ce qui ne va pas. En regroupant les informations sur les risques et les mesures de protection au même endroit, on garantit un suivi plus simple et plus efficace.

Exercice 3 Repérer l'utilisation des données à caractère personnel

1) Lorsqu'un utilisateur saisit des données personnelles (nom, adresse e-mail, historique d'achats, etc.) sur le site castorama.fr, ces informations peuvent être :

- utilisées pour identifier l'utilisateur et gérer son compte,
- partagées avec d'autres sociétés appartenant au même groupe,
- exploitées à des fins d'analyse ou d'études.

Cela signifie que les données ne restent pas exclusivement chez Castorama. Elles peuvent être transmises à d'autres entités et utilisées dans le cadre d'analyses.

2) Non, l'extrait seul ne permet pas de conclure que la confidentialité des données n'est pas respectée. Il est simplement indiqué que les données peuvent être partagées avec des tiers, mais aucune information n'est donnée sur les mesures de protection mises en place (par exemple, chiffrement, restrictions d'accès, etc.). Pour juger du respect de la confidentialité, il serait nécessaire de connaître les dispositifs de sécurité adoptés par Castorama.

Exercice 4 Traitement et risques sur les données à caractère personnel

1) Les données personnelles peuvent être traitées à différentes étapes :

Collecte : par exemple via un formulaire en ligne, des cookies lors de la navigation, ou une carte de fidélité.

Stockage : elles sont ensuite enregistrées dans des bases de données ou sur les serveurs de l'entreprise.

Diffusion : elles peuvent être utilisées dans des campagnes marketing ou partagées avec des partenaires commerciaux.

2) Une fois les données collectées, plusieurs opérations peuvent être effectuées :

Elles sont enregistrées puis conservées dans des systèmes organisés (comme des bases de données).

Elles peuvent être analysées, notamment à des fins statistiques ou marketing.

Certaines données peuvent être transmises à des partenaires ou sous-traitants.

Enfin, elles sont soit supprimées, soit rendues anonymes lorsqu'elles ne sont plus utiles.

3) Pour respecter la protection des données personnelles, certaines règles doivent être suivies :

Il faut d'abord obtenir le consentement des personnes concernées.

Il est essentiel de respecter le RGPD.

Les données doivent rester confidentielles, fiables et accessibles uniquement aux personnes autorisées.

Les utilisateurs doivent pouvoir consulter, corriger ou supprimer leurs données.

Et surtout, seules les données nécessaires doivent être collectées.

4) En cas de non-respect de ces règles, plusieurs conséquences peuvent survenir :

L’entreprise peut recevoir une amende.

Des personnes concernées peuvent demander des compensations.

Et au-delà de l’aspect légal, cela peut nuire à l’image de l’entreprise et faire perdre la confiance des clients.

Exercice 5 Dissocier les notions de sécurité et de sûreté informatique.

Situation	Impact sur la Sécurité	Impact sur la Sûreté	Justifications
Tous les serveurs sont inaccessibles à cause d'une inondation dans la salle technique.		✔	**L'inondation est un phénomène naturel, donc c'est une menace non intentionnelle.**
Les informations d'un hôpital deviennent illisibles à cause d'une attaque de type ransomware.	✔		**Cette situation résulte d'une attaque volontaire et malveillante.**
Le contenu du site web d'une entreprise est modifié par des personnes malveillantes durant le week-end.	✔		**Il s'agit d'une action délibérée et malveillante.**
Une surcharge électrique temporaire causée par des travaux dans les locaux entraîne une panne des routeurs.		✔	**Il s'agit d'un incident accidentel lié à l'environnement.**

Exercice 6 Identifier les données à caractère personnel

Données	Caractère Personnel	justifications
Le nom de la marque Carrefour	**NON**	Il s'agit d'une entreprise, pas d'une personne physique.
L'adresse e-mail professionnelle d'un directeur informatique	**OUI**	Cette adresse permet d'identifier directement une personne physique.
Une photo publiée sur un réseau social	**OUI**	La photo peut être utilisée pour reconnaître la personne.
Une vidéo de présentation professionnelle envoyée dans le cadre d'un recrutement	**OUI**	La vidéo peut servir à identifier la personne.
Les coordonnées GPS fournies par un smartphone	**OUI**	Quelqu'un ayant accès à ces données pourrait localiser la personne.
Le groupe sanguin d'un patient enregistré dans la base de données d'un médecin	**OUI**	Le groupe sanguin est associé à un dossier personnel nommé.
Les images issues de la vidéosurveillance d'un datacenter	**OUI**	Les images filmées peuvent permettre d'identifier les individus.
Le numéro d'enregistrement au registre du commerce d'une société	**NON**	Ce numéro correspond à une entreprise, pas à une personne physique.
Le numéro de sécurité sociale d'un employé mentionné sur sa fiche d'embauche	**OUI**	Ce numéro est un identifiant unique lié à une personne physique.

Conclusion

Ce TP m’a aidé à mieux comprendre les risques associés aux données personnelles et l’importance de mettre en place des mesures de sécurité adaptées. J’ai appris à distinguer sécurité et sûreté, à identifier les données sensibles et à réfléchir à des solutions pour les protéger. Ces compétences me seront utiles dans n’importe quel contexte professionnel.